34. (New) A system for allowing a smart card issuer to securely delegate to a third party the download of an applet to a smart card, said system comprising:

an external device associated with said third party, said external device capable of transferring said applet to said smartcard, wherein said applet is associated with said issuer and said applet is transferred by said third party as delegated by said information owner;

said smart card including instructions configured to initiate an acknowledgment process that produces a digital signature responsive to said transferred applet and a cryptographic key stored on said smart card, and send said digital signature to said issuer for validation by said issuer.

35. (New) The system of claim 34, wherein said acknowledgment process utilizes a symmetrical DES algorithm based on said cryptographic key.

36. (New) The system of claim 35, wherein said DES algorithm is a triple-DES algorithm.

37. (New) The system of claim 34, wherein said acknowledgment process utilizes a public-key encryption algorithm.

REMARKS

In the Office Action mailed July 11, 2002, the Examiner rejected pending claims 1-33. The present Amendment cancels claims 2, 5, 6, 10, 17, 18, 20, 21, 28, 29, and 30-33 without disclaimer, amends claims 1, 3, 4, 11, 13-16, 19, and 24-27, and adds new claims 34-37. As a result, claims 1, 3, 4, 7-9, 11-16, 19, 22-27, and 34-37 remain pending in the present application (3 independent claim, 23 claims total). No new matter has been added by this Amendment. Reconsideration is respectfully requested in light of the following Remarks.

A. Claim Rejections -- 35 U.S.C. § 102

Claims 1-8, 10-12, and 19-22 stand rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Pat. No. 6,105,008, issued to Davis et al. (the "Davis reference"). These rejections are respectfully traversed. Generally, as discussed in further detail below, the Davis reference fails to disclose, suggest, or teach one or more elements of independent claims 1 and 19 as amended and the various dependent claims depending therefrom. Furthermore, as claims 2, 8, 10, 20, and 21 have been canceled without prejudice, the Examiner's rejections regarding these claims are rendered moot.

The Davis reference generally discloses a network-based system used to reload stored-value smart cards. The architecture of the system includes a number of servers that coordinate to load and use a smart card for payment of goods and services purchased on-line over the Internet, including a payment server, a client terminal (which interfaces with the smart card), and a merchant server. Figures 18A-18D set forth a flowchart which, in conjunction with Figure 5, discloses a method for loading of value onto a card. The method disclosed in the Davis reference indeed involves the transfer of data (specifically, data representing monetary funds) between and among the three parties shown in Fig. 5, and involves the generation and transmission of some type of "acknowledgement." However, the components and flow disclosed by the Davis reference vary greatly from that which is recited in claims 1 and 19 as amended.

For example, the Davis reference does not disclose a system wherein the data is "transferred by said external device as delegated by said information owner" as variously recited in the claims as amended. That is, the transfer of data disclosed in the Davis reference is not delegated, but is merely initiated by the User himself (see step 871 in Fig. 18A), after which the

client terminal (which interfaces with the smart card) issues the load request to the load server (step 878 in Fig. 18A). In contrast, the present invention, as embodied in the pending claims, involves the delegated download of software in a way which is essentially transparent to the User of the smartcard. Specifically, the data (specifically, the "software") is transferred "as delegated by" the information owner (e.g., the issuer) as recited in claims 1, 9, and 34.

In addition, the Davis reference fails to disclose the transfer of "software" and the transmission, to the information owner, of a subsequently generated "verifiable acknowledgement of the transferred software" as recited in the pending independent claims. That is, the Davis reference exclusively deals with the secure transfer of information related to a monetary amount, which is a simple scalar value. The present invention relates to the transfer of software instructions and the generation of an acknowledgment based on the content of those instructions.

Furthermore, the Davis reference does not disclose a system wherein the information is "associated with the information owner" as recited in the independent claims. The Davis reference involves the transfer of funds from the payment server (item 206 in Fig. 5) to the merchant server (item 208 in Fig. 5); however, the monetary amount is not "associated with" the merchant server in the sense used in the present application. That is, the merchant server of Davis is not an "information owner" in the way the card issuer is the information owner of the transferred software delegated to the third party ("the external device") as recited in pending independent claims 1 and 19.

In summary, the Davis reference fails to disclose, suggest, or teach one or more elements of independent claims 1 and 19 as amended and the various dependent claims depending

therefrom. Accordingly, Applicants respectfully request that the Section 102 rejections be withdrawn.

B. Claim Rejections -- 35 U.S.C. § 103

Claims 9, 13-18, and 23-33 stand variously rejected under 35 U.S.C. § 103(a) as being unpatentable over the Davis reference in view of one or more of:

i) U.S. Pat. No. 5,590,038, issued to Pitroda et al. (the "Pitroda reference");

ii) W. Rankl and W. Effing, SMART CARD HANDBOOK (1997) (the "Rankl reference"); and

iii) Schnable, *A New High-Security Multi-Application Smart Card*, International Smart Card Conference (2000) (the "Schnable reference").

Applicant respectfully traverses these rejections and submits that no combination of the cited reference and prior art of record would include each and every element of the pending claims.

1. *Claims 9, 13, and 23-24*

Claims 9, 13, and 23-24 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over the Davis reference in view of the Patroda reference. These rejections are respectfully traversed.

Patroda relates to a "universal transaction card" ostensibly capable of serving as a number of different credit cards, bank cards, and the like. The Examiner cites Patroda in support of the argument that it would have been obvious to "expand the capability of the Davis invention" to PDAs and other such information devices. Applicant respectfully submits that, even to the extent that the Patroda reference discloses the use of PDAs, it does not disclose the use of PDAs in the

context of secure software download as recited in claim 9 as amended. In this regard, the arguments presented above with respect to differentiating the Davis reference also apply to the Patroda reference. As a result, a combination of the Patroda reference and the Davis reference would not result in the system as claimed in independent claim 9 as amended, nor does either reference include a motivation to combine the references.

Accordingly, Applicant respectfully requests that the Section 103 rejections be withdrawn with respect to claims 9, 13, and 23-24.

2. Claims 14-18, and 25-29

Claims 14-18 and 25-29 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over the Davis reference in view of the Rankl reference and the Schnable reference.

The Rankl reference generally discloses smart card file management (pages 217-219) including a verification procedure as outlined in Figure 7.44 of the Rankl reference. Similarly, the Schnable reference discloses various file and data management schemes. The Examiner argues that the Rankl and Schnable references teach that "operating system, applications (Applets, etc.) are routinely loaded into different information processing devices. . . ."

Even if the Rankl and Schnable references could be cited for generally disclosing the loading of applications and the like, these references, even when combined with the Davis reference, fail to disclose each and every element of independent claim 9 as amended. For example, reiterating the arguments presented above with respect to differentiating the Davis reference, no combination of the prior art of record discloses "transferring of software" with the production of "a verifiable acknowledgment of the transferred software" as "delegated by the information owner" as recited in the independent claims.

As claims 17, 18, 28, 29 have been canceled without disclaimer, the Examiner's rejections regarding these claims have been rendered moot. Accordingly, Applicant respectfully requests that the Section 103 rejections be withdrawn with respect to the pending claims.

3. Claims 30-33

Claims 30-33 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over the Davis reference in view of the Pitroda reference. These rejections are respectfully traversed. Nevertheless, as claims 30-33 have been canceled without disclaimer, these rejections are rendered moot.

In accordance with the above, Applicant reiterates that no combination of the cited references and prior art of record would include each and every element of any of the pending claims as amended. As such, Applicants do not need to address in detail the fact that there is no motivation or suggestion to combine the references. Applicant therefore requests that all Section 103 rejections be withdrawn with respect to the claims as amended.

C. Conclusion

In view of the above remarks, Applicants respectfully submitted that the foregoing remarks fully address the Examiner's objections, and that all of the pending claims comply with 35 U.S.C. § 112, are patentable over the art of record, and are in condition for allowance.

Attached hereto is a marked-up version of the changes made to the specification and claims by the present Amendment. The attached page is captioned "Version with markings to show changes made."

A Notice of Allowance respecting all pending claims is earnestly solicited. Should the Examiner wish to discuss any of the above in greater detail, then the Examiner is invited to telephone the undersigned at the Examiner's convenience.

Respectfully submitted,

Date October 11, 2002

By _____
Daniel R. Pote
Reg. No. 43,011

SNELL & WILMER, L.L.P.
One Arizona Center
400 East Van Buren
Phoenix, Arizona 85004-2202
(602) 382-6325

1220024.1

Version with markings to show changes made

In the Claims:

Claims 2, 5, 6, 10, 17, 18, 20, 21, 28, 29, and 30-33 are canceled without disclaimer or prejudice to the filing of one or more continuations or divisionals based on the subject matter of these claims.

The following claims are amended as indicated:

1. (Amended) A system for authenticating [downloading] download of [information] software to an information device, comprising:

[a. said information device;]

[b.] at least one external device capable of transferring [blocks of information] the software to said information device, wherein the [information blocks] software [belong to] is associated with an information owner remote from said external device, and wherein said software is transferred by said external device as delegated by said information owner; and

[c.] said information device configured to perform an acknowledgment process, wherein said acknowledgment process produces a verifiable acknowledgement of the transferred [information] software and sends said verifiable acknowledgement to said information owner for validation by said information owner.

3. (Amended) The system of Claim [2] 1, wherein [the] said verifiable acknowledgment can only be interpreted by [the] said information owner.

4. (Amended) The system of Claim [2] 1, wherein [the] said verifiable acknowledgment is a digital signature uniquely related to [the] said transferred [information] software.

11. (Amended) The system of Claim [1] 4, wherein said digital signature [acknowledgment process] is produced using a cryptographic key resident on said information device.

13. (Amended) The system of Claim 1, wherein said [information download] software comprises [is] new [information] instructions to be stored on said information device.

14. (Amended) The system of Claim 1, wherein said [information download] software is an update of existing [information] instructions stored on said information device.

15. (Amended) The system of Claim 1, wherein said [information download] software is a deletion of existing [information] instructions stored on said information device.

16. (Amended) The system of Claim 1, wherein said [information download] software comprises an applet.

19. (Amended) A method for an information owner to download [information] software to an information device, said method comprising the steps of:

a. the information owner [initiating] delegating, to a third party, download of said [information] software [download] to the information device; and

b. the information device computing an acknowledgment of said download of said software;

c. the information device making [the] said computed acknowledgment available to [a validating party] the information owner; and

d. the validating party verifying the computed acknowledgment.

24. (Amended) The method of Claim 19, wherein said [information download] software is new [information] instructions to be stored on said information device.

11. (Amended) The system of Claim [1] 4, wherein said digital signature [acknowledgment process] is produced using a cryptographic key resident on said information device.

13. (Amended) The system of Claim 1, wherein said [information download] software comprises [is] new [information] instructions to be stored on said information device.

14. (Amended) The system of Claim 1, wherein said [information download] software is an update of existing [information] instructions stored on said information device.

15. (Amended) The system of Claim 1, wherein said [information download] software is a deletion of existing [information] instructions stored on said information device.

16. (Amended) The system of Claim 1, wherein said [information download] software comprises an applet.

19. (Amended) A method for an information owner to download [information] software to an information device, said method comprising the steps of:

a. the information owner [initiating] delegating, to a third party, download of said [information] software [download] to the information device; and

b. the information device computing an acknowledgment of said download of said software;

c. the information device making [the] said computed acknowledgment available to [a validating party] the information owner; and

d. the validating party verifying the computed acknowledgment.

24. (Amended) The method of Claim 19, wherein said [information download] software is new [information] instructions to be stored on said information device.

25. (Amended) The method of Claim 19, wherein said [information download] software is an update of existing [information] instructions stored on said information device.

26. (Amended) The method of Claim 19, wherein said [information download] software [is a] overwrites [deletion of] existing [information] instructions stored on said information device.

27. (Amended) The method of Claim 19, wherein said [information download] software comprises an applet.

34. (New) A system for allowing a smart card issuer to securely delegate to a third party the download of an applet to a smart card, said system comprising:

an external device associated with said third party, said external device capable of transferring said applet to said smartcard, wherein said applet is associated with said issuer and said applet is transferred by said third party as delegated by said information owner;

said smart card including instructions configured to initiate an acknowledgment process that produces a digital signature responsive to said transferred applet and a cryptographic key stored on said smart card, and send said digital signature to said issuer for validation by said issuer.

35. (New) The system of claim 34, wherein said acknowledgment process utilizes a symmetrical DES algorithm based on said cryptographic key.

36. (New) The system of claim 35, wherein said DES algorithm is a triple-DES algorithm.

37. (New) The system of claim 34, wherein said acknowledgment process utilizes a public-key encryption algorithm.